Hezballah, Israel, and Cyber PSYOP

By Timothy L. Thomas

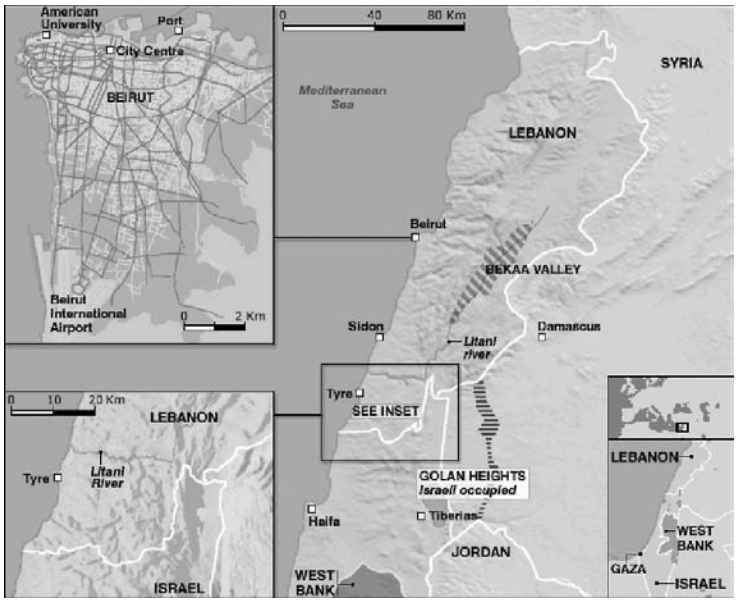
Editorial Abstract: ***The author analyzes the evolving phenomenon of cyber psychological operations, examining their application in the recent Israeli campaign against Hezballah. He describes CYOP forms and contents, and how these capabilities enhance both insurgent and friendly influence operations.***

Introduction

Parties on both sides of the recent fighting in Iraq, Afghanistan, and Lebanon have used cyber technologies to their advantage. Of course, this is nothing new. Tanks, planes, and soldiers have been uploaded with a host of cyber/information technologies for the past two decades at least. These technologies have increased the precision and lethality of weaponry, the situational awareness of the soldier, and the overall efficiency of operations.

However, an evolving cyber phenomenon is underway: the concept of cyber psychological operations (CYOP, pronounced "PSYOP")—which are cyber operations (those that use the computer chip) that aim to directly attack and influence the attitudes and behaviors of soldiers and the general population. While armies continue to compete in digital battlespace, local populations are now caught up in digital influence space battles. As a result armies can no longer stand between an enemy and the public as they once did. CYOP is also awash with "unintended consequences," since we are only now starting to understand what degree of influence, persuasion, deception, and mobilization the cyber environment offers. For example, mobile (cell) phones became "tools for citizen journalism" in Lebanon since they provided people the capability to transmit audio, video and photographs by short message service. Such contributions from "the street" carry their own form of psychological persuasion.

CYOP is characterized by speed, precision, and creativity. Speed is recognized due to the quickness of the message-response mechanism. An incident happens and is reported on the Internet, or via cell phone or video messaging, before legitimate news services can adjudicate its authenticity. Notably, these message have infinite—yet precise—reach (some call CYOP precision guided messages 'PGMs'). We can target friendly or enemy soldiers and populations with equal ease. Plus, creativity is an emerging issue. Technologies offer the ability to update time tested PSYOP techniques with new applications not tried or tested.



The physical battlespace. (Univ. of Texas/BBC)

The cyber element enables traditional psychological operations (PSYOP) such as loudspeakers and leaflets to penetrate not just a few miles into enemy territory, but to intrude directly and pervasively into the local populations' homes or across continents. The cyber element does so privately and quietly, invading not only computers and cell phones but the psychological well-being of the population as well. Local citizens on both sides of the Lebanese-Israeli conflict are victims of an intense propaganda and counterpropaganda campaign, for the maintenance of public and international support.

This article will investigate the emerging CYOP phenomena and its impact on the shape and outcome of future conflict. Please keep in mind this is an emerging and sensitive issue that is only beginning to be understood. Therefore, the issues presented represent only some initial thoughts and examples. Only further research will indicate how far this phenomenon has progressed and what eventual utility and capability it will offer future combatants.

Developments

For many years, at least until the late 1980s, PSYOP was usually associated with leaflets, rumors, loudspeakers, fake or gray news reporting, and deception. While the form of these old methods has

lived on into the cyber age, the methods and range of distribution—as well as the intended targets—have changed dramatically. New technologies have had totally unexpected consequences.

With regard to general cyber technologies, one can recall the recent August 2006 drinking incident involving actor Mel Gibson. The drunken Gibson uttered some ethnic slurs that a New York media firm gave away as a cell phone ring tone, the latter a popular cyber technology. An even more infamous ring tone incident in 2004 involved the President of the Philippines. Again, the incident speaks volumes about unintended consequences of the cyber age.

Philippine President Gloria Macapagal Arroyo, running for reelection, was talking with Commissioner of Elections Virgilio Garcillano in May 2004, before the election results were announced. Unaware the conversation was being tape recorded, she said "Hello Garci…will I win by one million votes?" When she found out that someone had recorded the phone call, Arroyo declined to allow local media to play the tape. In turn the tape quickly made its way onto activist websites and found use as a ring tone on cell phones, simply stating "Hello Garci?" Thus, while shopping in Manila or sitting on a plane, people were soon bombarded with the "Hello Garci…" ring tone.

Government authorities said the recording was made with an illegal wire tap, and was doctored. Other authorities said it was part of a plot against the president. On 28 June Arroyo admitted she had talked with Garcillano in a lapse of judgment. Thus ring tones, now used to embarrass people or to become a medium for political message delivery, may have unimaginable future uses as an attitude and behavior modifier.

Another unintended use of a cell phone may soon be tied to developments with specific audible tones or frequencies. Some websites advertise that a certain frequency is usually not detectable to people over the age of 30, while those younger than 30 can hear the frequency. The consequences are difficult to imagine. Are we to be segregated into technological groups based on age if the report is correct? Will some soldiers be able to hear a message and others won't? Will this impact how we construct forces? Further, can the sound be incorporated as a ring tone audible only to young people?

Similar developments are affecting the traditional PSYOP field dedicated to the use of leaflets and loudspeakers. During the recent fighting in Lebanon, the site http://beirutspring.blogspot.com reported that, in addition to the normal leaflet delivery "propaganda bombs," the Israeli's were using "E-flets." What is an E-flet? It is a leaflet type message that appears on the Internet, usually through URL links to a website. In one case, a website gave the appearance of being Lebanese in content (a red, green, and white Lebanese flag). It was accompanied by bombastic patriotic statements to rise against Hezballah. But the site had a +881 satellite number to call instead of a Lebanese number, and the server name was reportedly NS.BARAK.NET.IL. That is, this was probably an Israeli site to which one could call and report information. The site further guaranteed anonymity plus a cash deal.

"News doesn't always have to be fake to influence attitudes and behavior."

The loudspeaker has also been technologically updated in ways never imagined. The days of shouting at one another over cease fire lines or to encourage one side to surrender still exist, but these have been supplemented by the silent loudspeaker—the text message. Text and voice mail messages on mobile phones warned residents of Tyre in southern Lebanon to leave or risk being killed. This means the message is precision guided, just like high-tech weaponry. Coalition forces reportedly used the same method before their Match 2003 advance into Iraq. Their aim was to change the attitudes and behavior of Iraqi commanders by enticing them to defect or simply to go home and not fight. This means silent loudspeakers can potentially impact a campaign and be delivered at continental distances from the fight. Further, specific cell phone towers can become pieces of "key mental terrain," since some need to be left up and operating to text key population elements, while others can be shut down or destroyed.

Hizballah symbol.
(Terrorist Knowledge Base.org)

According to another report, the Israeli Defense Force (IDF) in Gaza are using similar phone messages. The Jerusalem Post reported on 27 July that nearly 1,000 residents of Gaza had listened to a recorded IDF message warning them not to harbor operatives or hide weapons. An Hamas government spokesman stated the Israeli intent was to drive people from their homes, paralyze the government, and demoralize the population.

Rumors, another traditional PSYOP technique, are difficult to spread unless you understand how to get into a groups mental "circle of influence." In Lebanon much of the information digested by the general population comes from radio, TV and newspaper reports. Taking a radio stations electronic broadcasts hostage and inserting one's own messages is not a difficult proposition in this day and age, and such activities occurred in Lebanon. One report in *The Guardian* noted that a local radio station "suddenly had reports broadcast from the Israeli government's

point of view." Cell phone images from "the street" also circulated and impacted on the "circle of influence."

Gray or fake news can be inserted quite easily in the cyber age. For example, mobile phones can be the medium through which to send regular messages—in the form of news updates—to discredit leaders or offer a different point of view on the fighting. Some mobile phone messages in Lebanon were headlined with the title "news." But recipients did not find customary news: instead they found news from the Israeli viewpoint. In addition, the Israelis resurrected a Voice of Lebanon radio station on frequency 103.7 Mhz. While not mentioned in the article, Voice of Lebanon's reporting could easily be inserted into mobile phone messages, if the former is ever blocked.

News doesn't always have to be fake to influence attitudes and behavior, of course. *The Daily Star*, a digital version of a Lebanese paper, had a few sentences at the start of its paper that said "Help Lebanon. Send a letter to your government representative. Download a sample letter." The last sentence linked to the letter and offered any Lebanese or foreign reader to download, fill in the blanks, and send the message to a congressman or parliamentarian.

While all the above elements involve some sort of deception, this category merits further discussion. It is never clear at the start who is calling or who is posting a news bulletin. Only after the fact is it possible to sit back and consider what just occurred. Then one's own sense of reality—based on experience and common sense—must prevail and offer a "best guess" of what the recipient believes. Furthering this movement into the unknown are websites like YouTube, where people can post their own videos. People are often swayed by visuals: they can seem more real than mere words. Many individuals have posted their personal videos of the fighting in Lebanon and other areas. As one source noted: "In a matter of weeks, YouTube has become a video trash bin for a global audience to share firsthand reports, military strategies, propaganda videos, and personal commentary about a violent conflict as it unfolds…It is a disorganized bazaar of images that requires visitors to search for a specific topic; searches for both "Hezballah" and "Israel" yield hundreds of videos, some of them violently graphic, others not so serious."

Naturally these videos could have been produced with deception in mind. One is reminded of the Iraqi Army's 1991 Gulf War video, which showed a sign posted outside a destroyed military facility stating it was a "baby milk factory." Or, more likely, YouTube videos can offer personal comments on the war and an outpouring of the emotional rage people feel over what happens to them or their families. Emotional videos with no deception intended can also have strong psychological overtones.

According to Yonit Farago of www.timesonline.co.uk, there is also an intense monitoring and counterpropaganda campaign underway by Israeli supporters. Special software termed "megaphone" is used to alert Jewish students to anti-Israeli chat rooms or Internet polls. These students then attempt to influence the course of a debate or an opinion survey by marshalling friends and supporters to take part. This allows a place where "networks of US and European groups with hundreds of thousands of Jewish activists can place supportive messages." The Israeli government is supportive of this effort. According to Farago, diplomat trainees have been ordered to track websites and chat rooms.

"Hezbollah has demonstrated in its war with Israel that it can take technology from other countries, and quickly adapt it to the battlefield.

Iranian President Mahmoud Ahmadinejad developed his own strategic counterpropaganda campaign. He opened a blog site when the Hezbollah-Israeli fighting ended, asking readers (they could vote yes or no) "do you think the US and Israeli intention and goal by attacking Lebanon is pulling the trigger for another world war?" By not offering the same question with regard to Hezballah, he clearly influenced attitudes and perhaps behavior in the Arab world.

Terrorist Groups And Technology

Groups like Al-Qaeda and Hezballah have developed CYOP of their own sort. These groups try to change attitudes and behaviors through intimidation, cyber fear, or outright racial or religious hatred. Of course their CYOP is not just aimed outward, but is internal as well. It often targets the disaffected in the Middle East, attempting to recruitment those who feel disenfranchised. Coalition forces have not done as well in efforts to neutralize these terrorist/insurgent activities in Iraq and Afghanistan as one would expect. US IO doctrine is weak (in fact, almost nonexistent) on the issue of counterpropaganda, and this is reflected in coalition operations. One journalist writes, "The Professors of the University of Hezballah have just rocketed past all the theoretical thinkers at cushy US war colleges."

Cyber operations have provided Al-Qaeda and Hezballah with their own newspapers and distribution means—and these means are becoming quite professional in appearance. A July 2006 tape from Al-Qaeda leader Ayman al-Zawahiri had a semi-professional look as if it was produced by a CNN affiliate. In the background are huge photos and stage lights, and it appears that Zawahiri is reading from signs or perhaps even a Teleprompter. Al-Qaeda's personal news studio, As-Sahab, produced the video. The result is that Zawahiri appears to be speaking from a position of authority simply based on the environment created for his talk. The context is a far cry from being filmed in a cave with a rifle at the ready, as he was in the early days of his retreat into geographical obscurity. However, the cyber age ensures no one is ever really obscure if they don't want

to be. A video camera and outlet for the recording is all that is required.

Terrorists have as much access to Internet voice technology as anyone else in the world. Voice over Internet Protocol (VoIP) "allows you to make telephone calls using a broadband Internet connection instead of a regular (or analog) phone line." Some services let you call anyone with a phone number, whether local or long distance. This makes it much harder to find and track terrorist cells.

In the war with Israel, Hezballah demonstrated they can take technology from other countries and quickly adapt it to the battlefield. On 7 August 2006, the Israelis shot down a terrorist operated reconnaissance unmanned aerial vehicle (UAV). Utilization of these technological advances makes Hezballah appear stronger than it actually might be, which is another psychological aspect of technology.

Cyber mobilization and attacks on attitudes don't stop at the US border, either. According to the website of Laura Mansfield, who has appeared on CNN with Anderson Cooper, several sites on MySpace advocate jihadist activities. This enables terrorist groups to write their own E-flets against US targets. More dramatic was the discovery made by the private Illinois group called the Society for Internet Research in August. The group noted Web site Al-Manar (outlawed in the US) made a stopover in Austin, Texas during the Hezbollah-Israeli conflict. When Israeli warplanes bombed its facilities in Lebanon, Al-Manar set up shop on Austin's Broadwing Communications servers. Finally, on 11 August a jihadist website posted the following message: "The Global Media: A Work Paper for Invading the US Media, Prepared by Najd al-Rawi." The message explains how to do this work and what tools to use.

Analyst Ben Venske notes jihadi videos are another terrorist favorite. They are used for several specific purposes instead of the "organized bazaar" represented by YouTube. These are: as instructional material, to make

Traditional media delivery. (Defense Link)

statements, to produce tributes to suicide bombers, to highlight operations, and to produce internal training videos among other uses. As a result such videos, especially those produced on hostage situations or operational successes, produce a type of follow-on psychological attack. Again, in the cyber age, the unintended mental (stress, fear, etc.) consequences of videos and technologies (text messaging) could also be termed follow-on CYOP attacks.

The Hezballah Central Internet Bureau has reportedly taken the video issue a step further. It has developed the video game "Special Forces" that places contestants in operations against Israel. The game praises martyrs, and credits those who shoot Israeli politicians and others. However, there are also reports, of Christian digital games in which soldiers either "save" or kill an opponent. Two points are awarded for a save and one point for a kill. It seems such games will have an impact on young people's attitudes and behavior on both sides, as they become morally disengaged from their physical versus their virtual realities.

Hard Versus Soft CYOP

The use of CYOP may soon enter the phase of hard CYOP. Hard CYOP refers to the development and implementation of ways to not just affect attitudes and behaviors, but to shut down the brain via some means—frequencies, chemicals, or some other method, especially those of the non-lethal variety. The Russians have been leaders in this category. Analyst S. P. Rastorguyev, for example, began writing openly about this subject in the 1990s at the behest of the Russian Security Council. His task was to develop algorithms that would put suggestive influences into human heads via words or sound. These influences were known as "psycho viruses."

Other writers, both in China and Russia, have discussed putting frequencies into computer programs or conducting other activities that would affect the "headware" (neurons) of a user. In the journal *Contemporary Navy,* the Chinese described efforts at conducting mind control, using telepathy, and using secondary sound waves in the 3-17 Hz range, that allegedly shut down a human's ability to function. This article also described use of blinding lasers, weapons of sound, holograms, and "camouflage by transfiguration." Elements of this type of CYOP (especially the use of a sound wave weapon) would be instantly debilitating. They would challenge your ability to continue functioning as a human.

Conclusions

The age of CYOP is upon us. Now silent loudspeakers disguised as cell phones, PDAs, and mp3 players reside in our pockets. A recorded call on Lebanese telephones these days is "Hasan, have

you realized yet that the Israeli army is not as delicate as a spider's web? It's a web of steel that will strangle you!" The intended recipient is not just the Lebanese people but the leader of Hezballah, Sheik Hasan Nasrallah. CYOP has also shown up on Lebanese TVs where purportedly Israeli hackers are putting out warnings reading "Hezballah members beware!"

The CYOP impact on future war is clearer now, since we are able to watch and evaluate it as it unfolds in all shapes and sizes in Lebanon, Afghanistan, and Iraq. If these wars are any indicator, future wars will be personal, deceptive, civil-military, and involve worldwide recruitment. All of these items will be managed and performed by cyber elements. Yellow journalism may also become a real threat. The website Little Green Footballs recently demonstrated how a Reuter's reporter had manipulated images of his photo reports from the field. Photographer Adnan Hajj had virtually enhanced and pasted (using Photoshop) a plume of smoke with concentric circles, making it appear to come from a building destroyed by an Israeli airstrike. Hajj was dismissed by Reuters and all of his 920 photos were removed from Reuter's database.

We are also able to do something else in the cyber environment—evaluate the consequences. This is because recipients of the CYOP messages often provide their reactions either in online blogs or in personal Internet interviews. One thing is very clear: CYOP is not only personal—but persuasive in new ways—some more powerful than any earlier PSYOP attempts. CYOP strikes raw nerves in a different way than a leaflet, due to its targeting precision with all forms of communications—auditory, visual, and print. CYOP appears to be a very invasive form of PSYOP that allows no mental sanctuary.

Teenagers, those most intimate with cyber technology, will be as affected—if not more so—than their elders in a cyber environment. Middle aged and senior citizens, more skeptical and analytical based on a lifetime of exposure and familiarity with deceptive techniques, will still require the more immature but technologically advanced teenager to interpret meanings and impacts—much like a translator. Cyber language and techniques are confusing and a difficult medium in which to stay current. For example, teenagers cruise through blogs and sites like Zone-H, Digg This (or just Digg), Little Green Footballs, MySpace, FaceBook, and technorati with abandon. Such sites provide a very different insight into a conflict than newspapers or TV. Online populations can actually interact with the populace of the other side in a conflict. There are also growing instances of media and Internet stardom that we must monitor for deception. These are situations where it appears the reporter's name and the virtual images he/she is reporting are the center of attention, at the expense of the tragedy and its victims.

Young and blog-savvy: the face of the CYOP generation. (Defense Link)

We must develop ways to recognize new CYOP techniques as they arise, and monitor the consequences they bring with them. We must remain vigilant in particular for hard CYOP developments. Today Viagra and other spam type messages reach us quite easily from home and abroad, and luckily these are only soft "ad attack" CYOP. Will hard CYOP be able one day to reach us as easily? Terrorist groups have no moral dilemma using hard (frequency generated) messages. The Russian fear that researchers are intent on finding ways to control human consciousness may be just around the corner, if the terrorists have a say in the matter. Technological developments are moving that fast, and may contain several unintended consequences, beyond those that have already surprised us.

The general population is not only a favorite target of CYOP, but has become a self-generator or CYOP participant as well. For example, a subscriber recently used Google Earth to document military actions on both sides of the Israeli-Lebanese border. The subscriber's maps provided an instantaneous photo montage of potential military strategies, acting as an intelligence source for groups without satellite capabilities. As one description of the site noted, it contained "details on the action which occurred at the location and the casualties or damage resulting, and allows you to view the aerial photos and see what it looked like before the conflict." No current newspaper or TV report can currently replicate this type of updated, constantly reviewable data, conducted at one's own pace—although news outlets are moving in this direction.

CYOP can produce other psychological impacts as well. Not all of them are as neutral as Google Earth. Of greatest concern are hate propaganda, calls to arms and cyber mobilization. Of lesser but still notable concern is the impact of Internet-generated cyber fear. Gabriel Weimann, one of the most prolific and well-known authors on the terrorist use of the

Internet, has noted with regard to the cyber age that "From a psychological perspective, two of the greatest fears of modern times are combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat. Although cyberterrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the threat of terrorist bombs.

We must follow the CYOP phenomenon as it picks up momentum. Groups will initiate new and varied techniques, and everyone must be on guard to counter the unexpected. E-flets, silent loudspeakers, Google Earth, ring tones, and YouTube represent only the start of this phenomenon. Traditional PSYOP personnel will play a key role in uncovering the advantages offered by these technological advances, and then must creatively apply counters to them in warfare. CYOP can be private, silent, deceptive, intercontinental, and as full of hatred and prejudice as the initiator wants it to be—and all are issues that should concern us.

Notes

[1] Lysandra Ohrstrom, "Mobile Phones Play Key Role in Lebanon War," Daily Star, 16 August 2006, from *The Information Operations Newsletter*, Jeff Harley editor, Vol 6, No 18 (11-21 August 2006)

[2] "Sign of the Times," *Kansas City Star,* 4 August 2006, p. C1 (located in the header on the page).

[3] Dave Pugh, "Ring-Tone Revolution in the Philippines," http://mrzine.monthlyreview.org/pugh230705.html, downloaded on 31 July 2006.

[4] Sarah Toms, "Philippine Tape in Ringtone Craze," BBC News, downloaded from news.bbc.co.uk on 31 July 2006.

[5] Pugh.

[6] Google search Mosquito, adult-proof, and silent ringtones to read the positive and negative potential of this idea.

[7] "Israeli E-leaflets," downloaded from http://beirutspring.blogspot.com, 24 July 2006.

[8] Clancy Chassay, "Info War Goes Personal with Voicemail and Text Message," *The Guardian*, 24 July 2006.

[9] Associated Press, "New IDF Tactic: the Phone Call," *The Jerusalem Post,* 27 July 2006.

[10] Chassay.

[11] Ibid.

[12] The Daily Star, 1 August 2006, downloaded from www.daily star.com.lb.

[13] Sara Kehaulani Goo, "Videos about Mideast conflict now appearing on Internet site," *The Kansas City Star*, 26 July 2006, p. A12.

[14] Jonit Farago, "Israel Backed by Army of Cybersoldiers," www.timesonline.co.uk, downloaded on 31 July 2006.

[15] Ibid.

[16] "Doing His Blog: Populist President Goes Online," *The Guardian*, 15 Aug 06, downloaded from www.smh.com.au.

[17] John E. Carey, "Hezballah is Way Ahead. Again," *Peace Journalism*, 17 Aug 06, downloaded from peacejournalism.com.

[18] Information accessed at http://www.fcc.gov/voip and downloaded on 9 August 2006.

[19] CNN TV, 8 August 2006.

[20] See http://blog.lauramansfield.com/2006/05/18/teen-terror-on-the-web-jihadi-and-islamist-activi...

[21] Todd Bensman, "Hezballah Web Site Booted in Austin," Express-News Staff Writer, downloaded from www.freerepublic.com

[22] "Global Islamic Media Front Discusses Plan for Penetrating US Media," OSC Report in Arabic, 23 August 2006, contained in an e-mail to the author from FMSO analyst Kevin Freese.

[23] Ben Venske, "Evolution of Jihadi Video (EJV) V1.0," *Journal of Counterterrorism and Homeland Security International*, Vol. 12, No. 1, pp. 50-51.

[24] The game is offered at its own website, at http://www.specialforce.net/english/indexeng.htm.

[25] Author's meeting with S. P. Rastorguyev at a conference in Moscow, 1997.

[26] Associated Press, "This is the beginning of the cellular phone war," Ha'aretz, 8 August 2006.

[27] Ibid.

[28] Website for Little Green Footballs, www.littlegreenfootballs.com, accessed on 7 August 2006.

[29] "Reuters Says Mideast Photographer Doctored Shots," www.cnn.com, accessed on 8 August 2006.

[30] http://www.gearthblog.com/blog/archives/2006/07/israellebanon_c.html, Google Earth, posted by Frank Taylor 21 July 2006.

[31] Gabriel Weimann, *Terror on the Internet*, US Institute of Peace, 2006, p. 150.

Tim Thomas, LTC, US Army, Retired, served as a Soviet/Russian Foreign Area Officer. His assignments include brigade S-2 and company commander in the 82d Airborne Division, and the Army Russian Institute. He has done extensive research and publishing in the areas of peacekeeping, IO, and PSYOP. He currently serves as a Senior Analyst in the Foreign Military Studies Office, Ft Leavenworth. He holds a BS from West Point, and Master of Arts from USC.